DRMS-D 5210.4

DRMS-IZ

28 Feb 97

APPOINTMENT OF FUNCTIONAL DATA OWNERS/SYSTEM RESOURCE OWNERS
(Supplementation is prohibited.)

A. REFERENCES.

1. DLAR 5200.17, Security Requirements for Automated Information and Telecommunications Systems.

2. DRMS-D 5200.1, Processing of Requests for Computer User Accounts.

3. DRMS-I 5200.1, Processing of Requests for Computer User Accounts.

4. DoD 5200.2-R, Appendix K, ADP Position Categories and Criteria for Designating Positions.

5. DoD Directive 5200.28, Security Requirements for Automated Information Systems (AISs).

6. DRMS-D 5210.5, Development of DRMS Functional Data and System Resources Access Policies.

B. PURPOSE. This directive describes the method for the appointment of Functional Data Owners/System Resource Owners. It standardizes specific actions and required documentation for all locations.

C. APPLICABILITY AND SCOPE. This directive applies to HQ DRMS, the directorates of Operations East and West, Europe, the International Sales Office (ISO), and all Defense Reutilization and Marketing Offices (DRMOs), Foreign Nationals and all Military personnel assigned to Defense Reutilization and Marketing Service (DRMS).

D. DEFINITIONS.

1. ACCESS ACCOUNT ADMINISTRATOR (AAA). Person or persons responsible for the connecting of user accounts to identified systems after all approvals have been received for access.

2. ADP-II. Those positions in which the incumbent is responsible for the direction, planning, design, operation, maintenance of a computer system or AIS and whose work is technically reviewed by a higher authority of the ADP-I category to insure the integrity of the system.

3. AUTOMATED INFORMATION SYSTEM (AIS). An assembly of computer hardware, software, and/or firmware configured to collect, create, communicate, compute, disseminate, process, store, and/or control data or information. Networks are considered to be AIS also.

4. AUTOMATED INFORMATION SYSTEM SECURITY OFFICER (AISSO). The focal point for information concerning the secure design and development of an AIS. This individual, in coordination with the Data Owners/System Resource Owners, determines the security controls needed to protect the information being processed. The AISSO

conducts the security requirements analysis for an AIS prior to development, supports the Information System Security Officer's (ISSO) testing and evaluation effort, and documents the results in the supporting documentation for AIS accreditation.

5. CONTRACTOR. Person employed by private industry who performs duties in accordance with government contract.

6. DATA. A noncontextual representation of facts, concepts, and instructions in a defined format and structure which permits processing by humans or machines to derive information. Representations of people, places, things, concepts, events, or activities in a defined format and structure from which information may be derived.

7. DATA OWNER (also RESOURCES OWNER): The individual(s) responsible for approving access requests and making decisions about the protection and use of sensitive information and resources. Data owners and resources owners are the personnel responsible for the business functions supported by the AISs.

8. DENIAL OF ACCESS/SERVICE. Action or series of actions that prevent any part of a system from functioning in accordance with it intended purpose. Also includes disapproval of request for access to data.

9. DESIGNATED APPROVING AUTHORITY (DAA). The agency or activity focal point with the authority to grant AIS accreditation and security software certification, and to accept whatever minimal or residual risk may be left after the implementation of countermeasures.

10. FUNCTIONAL AWARENESS. Knowledge of the workings of all data associated with the assigned AIS.

11. FUNCTIONAL DATA OWNER/SYSTEM RESOUCE OWNERS (FDO/SRO). Same as Data Owners/System Resource Owners.

12. FOREIGN NATIONAL (FN). Person of foreign country nationality. Not necessarily employed by the U.S. Government.

13. INFORMATION SECURITY SYSTEM MANAGER (ISSM). The activity focal point for advising the Designated Approving Authority on AIS security matters. In his/her operational capacity, the ISSM assists in the establishment, implementation, and review of AIS security programs. The ISSM makes recommendations, maintains liaison and coordination with other organizations, and assures compliance with security policies.

14. PRACTICAL AWARENESS. Actively engaged in or knowledge of the functional working of an AIS.

15. SUPPLEMENTAL ASSIGNMENT DATA SHEET (SADS). Explains any additional duties that may be assigned outside of position description. Should be attached to employee permanent record.

E. POLICY.

1. Appointment of Data Owners/System Resource Owners.

a. Primaries and Alternates Data Owners/System Resource Owners must be appointed.

b. Contractors, students, and part-time/temporary employees may not be appointed as DATA Owners/System Resource Owners.

c. Foreign nationals may not be appointed as DATA Owners/System Resource Owners without approval from DLA on existing policy with the exception of employees already occupying current positions.

d. Persons considered for the position of Data Owners/System Resource Owners must at a minimum be on an ADP-II position. See reference A5.

e. Data Owners/System Resource Owners must have a functional awareness of data and resources they are responsible for.

f. Data Owners/System Resource Owners must have an insight of data/resources sensitivity and integrity.

g. DRMO Chiefs are considered the data owners of the sites systems; as such, a appointment letter is not required for them.

2. Letter of Appointment. Appointment must be in writing except as in E.1.g. Enclosure 1 is an example of a formal appointment letter. A copy of this letter must be sent to DRMS-IZ Security and will be kept on file there.

3. DATA Owners/System Resource Owners. The Data Owners/System Resource Owners duties must be in direct compliance with reference A1, which follow the guidance for all Data Owners/System Resource Owners included in this directive.

4. Supplemental Assignment Data Sheet (SADS). Must be developed for each Data Owners/System Resource Owner and placed in their personnel files. (See enclosure 2.)

5. Ownership conflicts. Heads of Principle Staff Elements (PSEs) will designate data owners/resources owners. For all systems/applications, the owners will be the persons responsible for the business functions supported by the systems/applications. Some systems/applications support multiple PSEs and could possibly have multiple owners. Where conflicts arise over owner boundaries, the DLA Data Administrators are responsible for resolving those issues (see Reference A1, Encl. 16).

F. RESPONSIBILITIES

1. Defense Reutilization and Marketing Service (DRMS) Managers will:

a. Appoint Primary and Alternate Data Owners/System Resource Owners.

b. Issue Letter of Appointment to be sent to Primary and Alternate Data Owner/System Resource Owners with copy to DRMS-IZ security. (See enclosure 1.)

c. Notify DRMS-IZ Security in writing when Data Owners/System Resource Owners are to be changed or deleted.

d. Assure that the Data Owners/System Resource Owners meet all requirements of position.

e. Share equally the responsibility for the integrity of the data.

f. Assure SADS is attached to Data Owners/System Resource Owners Position Description. (See enclosure 2.)

2. Data Owners/System Resource Owners will:

a. Identify the functional/system resource access requirements and sensitivities of the information under their ownership and provide sufficient guidance to the AISSO to permit him/her to identify and prescribe security countermeasures needed.

b. Develop a formal access control policy to identify the user and/or user groups who shall be permitted access to the AIS/resources, the level of position

sensitivity required by users granted such access, the nature of the access (such as read-only), and with the assistance of the AISSO, the system compartments or domains to which the users shall be granted access.

c. Ensure dissemination of the access control policy to the ISSM and to all organizations using or operating the AIS/resources.

d. Ensure current status on policies is maintained.

e. Participate in AIS risk analysis and contingency planning efforts.

f. Notify requester in writing with explanation when there is a denial of access.

g. Ensure that all requests go through the established procedures and associated processing before approving access.

h. Forward approved request to Access Account Administrator with notation of approval.

3. Automated Information System Security Office (AISSO) will:

a. Serve as the focal point for information concerning the secure design and development of an AIS.

b. Fully comprehend the accreditation and certification processes outlined for data/resource.

c. Ensure the Data Owner/System Resource Owner understands the protection requirements for data/resource.

d. Review all changes and endorse all completed changes, certifying that the prevailing security protection has not weakened.

e. Be responsible for the accreditation review of accredited AISs.

f. Serve as Designated Approving Authority (DAA).

4. Access Account Administrator will:

a. Verify that all approvals have been received before assigning access. If not return for proper authorization.

b. Add account to the system following all rules that have been set for the proper administration of the system.

c. Send written notification to TASO stating userid, password assignment, return receipt and rules on the use of userids.

d. Keep on file all requests indefinitely or until one year after the system has been eliminated.

e. See that all deletions received from DRMS management are processed within 24 hour time period.

5. ISSM - Information Security System Manager will:

a. Advise the DAA on AIS security matters.

b. Assist in the establishment, implementation and review of AIS security programs.

c. Make recommendations, maintains liaison and coordination with other organizations, and assures compliance with security policies.

6. DLA Data Administrator is responsible for resolving conflicts over data ownership boundaries and/or access policy conflicts.

G. EFFECTIVE DATE AND IMPLEMENTATION.

1. This publication is effective and shall be implemented upon distribution.

2. Initial DATA Owner Appointment.

a. DATA Owners are selected by DRMS Management.
b. DATA Owner's and Management will discuss the responsibilities and duties as defined in DRMS-I 5210.5.
c. Assurances are made that Data Owners/System Resource Owners meet all requirements of position.

3. Data Owners/System Resource Owners assignment Documentation.

a. DATA Owners and/or System Resource Owners receives Letter of Appointment.
b. DRMS-IZ security receives copy of appointment letter.
Copy of letter may be faxed or mailed to DRMS-IZ via the following:

Fax to DSN 932-4115 or COM 616-961-4115.

Mail to DRMS-IZ, Security
74 Washington Avenue North
Battle Creek, MI 49017-3092

4. ACCEPTANCE PROCESSING. Upon acceptance of the Appointment Letter, DRMS Manager will assure that the Data Owners/System Resource Owners are furnished a copy of DRMS-D 5210.4, Appointment of Functional Data Owners/System Resource Owners and DRMS-D 5210.5 Development of DRMS Access Policies.

H. INFORMATION REQUIREMENTS. (Reserve for future use.)

BY ORDER OF THE COMMANDER

/s/
DOUGLAS W. YOUNG
LCDR, SC, USNR
Executive Officer

2 Encl.
1. Data Owners/System Resource Owners Appointment Letter (sample).
2. Supplemental Assignment Data Sheet (SADS) (sample)

Coordination: All HQ DRMS Directors, East/West Operations Deputy Commanders, Europe Region Commander.

Encl 1
DRMS-D 5210.4

EXAMPLE OF APPOINTMENT LETTER

FROM: (DRMS MANAGER)
DCN E-MAIL xxxxxx@xxxxx.xxxx.xxx

SUBJECT: Functional Data Owners/System Resource Owners Letter of Appointment

TO: John Doe (specific which: Data Owners or System Resource Owners - primary or
alternate)

1. Reference: DRMS-D 5210.4, Appointment of Functional Data Owners/System Resource Owners.

2. <Data Owners or System Resource Owners name>, <office symbol>, <standard logon identifier>, <e-mail address>, <phone number>.

3. The following AISs/System resources <whichever is applicable> are now the responsibility of the above appointed Functional Data Owners/System Resource Owners.

(examples: systems, datasets; anything dealing with computer permissions where access is required to be given)

a. _____

b. _____

4. This appointment becomes effective on <date>. You will carry out the duties and responsibilities as identified in the above reference.

<signed>

cc:
DRMS-IZ

SUPPLEMENTAL ASSIGNMENT DATA SHEET (SADS)

Organization Symbol_____

Employee_____

Pay Plan, Series, Grades_____

Current PD number_____

Date Duties assigned_____

DUTIES:

Above named has been appointed to the duties of Functional Data Owners/System Resource Owners. Responsible for supporting Agency security requirements and performing specific security duties which includes the granting of access to the above specified systems/datasets. Duties are in compliance with DLAR 5200.17.

- Adhere to the guidelines and procedures as directed by interoffice policies.
- Grant requests for computer access for employees assigned to their designated area of responsibility according to current access policies related to processing of requests for computer user accounts.
- Forward approved request to responsible area for data entry of request into system.
- Forward disapproved request to originators with explanation.
- Will ensure that all requests for DRMS employees go through the AURA system for approving access.
- Identify the functional access requirements and sensitivities of the information under their ownership and provide sufficient guidance to the AISSO to permit him/her to identify and prescribe security countermeasures needed.
- Develop a formal access policy to identify the users and/or user groups who shall be permitted access to the AIS, the nature of the access (such as read-only), and with the assistance of the AISSO, the system compartments or domains to which the users shall be granted access.
- Ensure dissemination of the access policy to the ISSM and to all organizations using or operating the AIS.
- Where the developed policy is inadequate or difficult to apply, authorize on a case-by-case basis access to files, programs, and data bases under their cognizance.
- Participate in AIS risk analysis and contingency planning efforts to ensure that appropriate protection is afforded the information in the event of system failure or increased risk to the automated environment.

_____
Supervisor